REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
03-03-2016	Final Report	8-Aug-2011 - 30-Jun-2014

4. TITLE AND SUBTITLE
Final Report: DURIP: Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure

5a. CONTRACT NUMBER
W911NF-11-1-0341

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
Patrick Traynor

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Georgia Tech Research Corporation
505 Tenth Street NW

Atlanta, GA 30332 -0420

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
59369-CS-RIP.17

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The recent and rapid expansion of cellular capabilities has created tremendous opportunities for new applications and services. From mobile banking and location- based services to the real-time streaming of music and video, cellular networks now provide advanced voice and data services to more than 4.5 billion subscribers around the world. When compared to the approximately one billion users who access the Internet each day through traditional means, cellular networks represent the only communication system available to a significant portion of the world's population and the next significant expansion in high-speed Internet connectivity. As we all grow increasingly

15. SUBJECT TERMS
Cellular, Mobile, Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Patrick Traynor
UU	UU	UU	UU		19b. TELEPHONE NUMBER 352-392-1200

Report Title

Final Report: DURIP: Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure

ABSTRACT

The recent and rapid expansion of cellular capabilities has created tremendous opportunities for new applications and services. From mobile banking and location- based services to the real-time streaming of music and video, cellular networks now provide advanced voice and data services to more than 4.5 billion subscribers around the world. When compared to the approximately one billion users who access the Internet each day through traditional means, cellular networks represent the only communication system available to a significant portion of the world's population and the next significant expansion in high-speed Internet connectivity. As we all grow increasingly reliant on such devices, the risk of security vulnerabilities in the mobile phones and their supporting infrastructure represents not just an inconvenience, but a tangible threat to the safety and security of societies around the world. A significant barrier to basic research in this arena is the absence of available infrastructures to conduct rigorous testing and experimentation. This has resulted in a reduced understanding of the cellular threat landscape as compared to traditional Internet.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received		Paper
03/03/2016	1.00	Adam Bates, Kevin R.B. Butler, Micah Sherr, Clay Shields, Patrick Traynor, Dan Wallach. Accountable wiretapping – or – I know they can hear you now, Journal of Computer Security, (06 2015): 0. doi: 10.3233/JCS-140515
03/03/2016	2.00	Patrick Traynor. Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services, IEEE Transactions on Mobile Computing, (06 2012): 0. doi: 10.1109/TMC.2011.120
03/03/2016	9.00	Chaitrali Amrutkar, Italo Dacosta, Patrick Traynor, Henry Carter. For your phone only: custom protocols for efficient secure function evaluation on mobile devices, Security and Communication Networks, (07 2014): 0. doi: 10.1002/sec.851
03/03/2016	14.00	Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, Patrick Traynor. One-time cookies, ACM Transactions on Internet Technology, (06 2012): 0. doi: 10.1145/2220352.2220353
03/03/2016	16.00	Chaitrali Amrutkar, Patrick Traynor, Paul C. van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers, IEEE Transactions on Mobile Computing, (05 2015): 0. doi: 10.1109/TMC.2013.90
TOTAL:	**5**	

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received		Paper
03/03/2016	3.00	Charles Lever,, Manos Antonakakis,, Bradley Reaves,, Patrick Traynor. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers, ISOC Network & Distributed System Security Symposium (NDSS). 24-FEB-13, . : ,
03/03/2016	4.00	Chaitrali Amrutkar, Matti Hiltunen, Trevor Jim, Kaustubh Joshi, Oliver Spatscheck, Patrick Traynor, Shobha Venkataraman. Why is my smartphone slow? On the fly diagnosis of underperformance on the mobile Internet, 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). 24-JUN-13, Budapest, Hungary. : ,
03/03/2016	5.00	Bradley Reaves,, Ethan Shernan,, Adam Bates,, Henry Carter,, Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the NetworkEdge, USENIX Security Symposium (SECURITY). 21-AUG-15, . : ,
03/03/2016	6.00	Arunabh Verma, Henry Carter, Patrick Traynor, Philip Marquardt. (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers, ACM Conference on Computer and Communications Security (CCS). 17-OCT-11, Chicago, Illinois, USA. : ,
03/03/2016	7.00	Saurabh Chakradeo, Bradley Reaves, Patrick Traynor, William Enck. MAST: Triage for Market- scale Mobile Malware Analysis, Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec). 17-APR-13, Budapest, Hungary. : ,
03/03/2016	8.00	Henry Carter,, Benjamin Mood,, Patrick Traynor, Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices, Proceedings of the USENIX Security Symposium (SECURITY). 21-AUG-15, . : ,
03/03/2016	10.00	Henry Carter, Charles Lever, Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices, the 30th Annual Computer Security Applications Conference. 08-DEC-14, New Orleans, Louisiana. : ,
03/03/2016	11.00	Italo Dacosta,, Mustaque Ahamad,, Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties, European Symposium on Research in Computer Security (ESORICS). 15-APR-12, . : ,
03/03/2016	12.00	Chaitrali Amrutkar,, Patrick Traynor, Paul van Oorschot. Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?, Information Security Conference (ISC). 04-JUL-12, . : ,
03/03/2016	13.00	Chaitrali Amrutkar,, Kapil Singh,, Arunabh Verma,, Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security, International Conference on Information Systems Security (ICISS). 05-DEC-12, . : ,
03/03/2016	15.00	Chaitrali Amrutkar, Patrick Traynor. Short paper: Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM). 19-OCT-12, Raleigh, North Carolina, USA. : ,

TOTAL: **11**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Patrick Traynor	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):.....	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

See attachment.

Technology Transfer

DURIP: Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure

W911NF-11-1-0341

Defense University Research Instrumentation Program (DURIP)
Army Research Office

Final Report

Patrick Traynor

Table of Contents

1. Abstract

The recent and rapid expansion of cellular capabilities has created tremendous opportunities for new applications and services. From mobile banking and location-based services to the real-time streaming of music and video, cellular networks now provide advanced voice and data services to more than 4.5 billion subscribers around the world. When compared to the approximately one billion users who access the Internet each day through traditional means, cellular networks represent the only communication system available to a significant portion of the world's population and the next significant expansion in high-speed Internet connectivity. As we all grow increasingly reliant on such devices, the risk of security vulnerabilities in the mobile phones and their supporting infrastructure represents not just an inconvenience, but a tangible threat to the safety and security of societies around the world. A significant barrier to basic research in this arena is the absence of available infrastructures to conduct rigorous testing and experimentation. This has resulted in a reduced understanding of the cellular threat landscape as compared to traditional Internet.

We proposed the procurement of a system that enables student researchers and faculty to evaluate threats against these classes of devices, thereby enhancing education and research in this important and rapidly developing area.

2. Equipment

The proposed grant was designed to cover a wide range of devices. We not only requested the purchase of a large number of mobile phones to support mobile application development, but also wireless base stations to create our own small-scale networks, and laptop-, desktop- and server-class machines to allow for writing software and data processing.

Mobile devices ended up being the most beneficial to the widest range of research projects. These systems were used to perform research on mobile malware, TLS and the mobile web, and core network security. Additionally, the mobile devices purchased as part of this grant were used to support our work on the DARPA PROCEED Program (AFRL FA8750-11-2-0211: Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation). We were also able to allow students working as part of the graduate course "Cellular and Mobile Network Security" to build Android applications as part of their course research projects.

Traditional computing resources (laptops, desktops and servers) were extremely valuable in developing software for these mobile devices. A number of our projects collected extensive amounts of data or required massive computing power (especially those related to DARPA PROCEED). Accordingly, we were able to perform such research duties only because of this infrastructure.

Lastly, we purchased two of the proposed five mobile base stations. Our first unit had dramatically limited functionality, and ended up being useful for only a short lifetime. Students used this device to build a small testbed in support of their class projects. We purchased a second device, from Range Networks, which offered dramatically expanded capabilities. However, because of spectrum limitations in the Atlanta downtown, we opted to purchase a Faraday box to ensure that our experiments did not interfere with legitimate signals in the area. This precaution prevented us from purchasing and deploying the additionally proposed items to create a larger network.

PI Traynor left Georgia Tech for the University of Florida in the Summer of 2014. Georgia Tech refused to allow PI Traynor to transfer the equipment, opting instead to require that all equipment remain there. PI Traynor was told that the equipment would be "surplussed" in spite of it having significant useful like remaining. Because PI Traynor retains adjunct status at Georgia Tech, he has been able to continue using some of the equipment; however, the Chair of the Department of Computer Science will need to be contacted for justification of early equipment expiration and any questions regarding the final budget.

3. Published Papers

This DURIP supported significant research activity, and directly resulted in the following published scientific papers:

Core Network Security

1. A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach, **Accountable Wiretapping -or- I Know They Can Hear You Now**, In Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS), 2012.

2. P. Traynor, **Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services**, IEEE Transactions on Mobile Computing (TMC), 11(6):983-994, 2012.

3. C. Lever, M. Antonakakis, B. Reaves, P. Traynor and W Lee. **The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers**, In Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS), 2013.

4. C. Amrutkar, M. Hiltunen, T. Jim, K. Joshi, O. Spatscheck, P. Traynor and S. Venkataraman, **Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet**, Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2013.

5. B. Reaves, E. Shernan, A. Bates, H. Carter and P. Traynor, **Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge** Proceedings of the USENIX Security Symposium (SECURITY), 2015.

6. A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach, **Accountable Wiretapping -or- I Know They Can Hear You Now**, Journal of Computer Security (JCS), 23(2):167-195, 2015

Mobile malware

7. P. Marquardt, A. Verma, H. Carter and P. Traynor, **(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers**, Proceedings of the ACM Conference on Computer and Communications Security (CCS), October, 2011.

8. Y. Nadji, J. Giffin and P. Traynor, **Automated Remote Repair for Mobile Malware**, Proceedings of the Annual Computer Security Applications

Conference (ACSAC), December 2011.

9. S. Chakradeo, B. Reaves, P. Traynor and W. Enck, **MAST: Triage for Market-scale Mobile Malware Analysis**, In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2013. (**best paper**)

Privacy-preserving Computation

10. H. Carter, B. Mood, P. Traynor and K. Butler. **Secure Outsourced Garbled Circuit Evaluation for Mobile Devices**, In Proceedings of the USENIX Security Symposium (SECURITY), 2013.

11. H. Carter, C. Amrutkar, I. Dacosta and P. Traynor, **For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices**, Journal of Security and Communication Networks (SCN), 7(7), p. 1165–1176, 2014.

12. H. Carter, C. Lever, P. Traynor, **Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices**, Proceedings of the Annual Computer Security Applications Conference (ACSAC), December 2014.

13. H. Carter, B. Mood, P. Traynor, and K. Butler. **Secure Outsourced Garbled Circuit Evaluation for Mobile Devices.** Journal of Computer Security (JCS), To Appear 2016.

TLS and the Mobile Web

14. I. Dacosta, M. Ahamad and P. Traynor, **Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties**, In Proceedings of the European Symposium on Research in Computer Security (ESORICS), 2012.

15. C. Amrutkar, P. Traynor and P. van Oorschot, **Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?**, In Proceedings of the Information Security Conference (ISC), 2012. (**best student paper**)

16. C. Amrutkar, K. Singh, A. Verma and P. Traynor, **VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security**, In Proceedings of the International Conference on Information Systems Security (ICISS), 2012.

17. I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor. **One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens**, ACM Transactions on Internet Technology (TOIT), 12(1), 2012.

18. C. Amrutkar and P. Traynor, **Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead**, Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2012.

19. C. Amrutkar, P. Traynor and P. van Oorschot, **An Empirical Evaluation of Security Indicators in Mobile Web Browsers**, IEEE Transactions on Mobile Computing (TMC), 14(5):889-903, 2015.

4. Conclusions

Cellular systems represent some of the most critical infrastructure in our modern world. Whereas some two billion people use the Internet daily, over six billion subscribers rely on telephony networks as their only access to digital communications. Accordingly, the security of these systems requires heightened attention from our security.

This grant has enabled a wide range of research projects that would not have been possible without this infrastructure. From expensive wireless interfaces and equipment to the back-end processing necessary to compute results over large data produced by our experiments, this funding has helped address critical questions about the reality and spread of mobile malware, the practicality of new techniques to prevent fraud and denial of service in core infrastructure, whether privacy-preserving computation is possible on mobile devices and the state of security in the mobile web.

Moreover, this work allowed for three PhD students (Italo Dacosta, Chaitrali Amrutkar and Henry Carter) the infrastructure they required to successfully complete their dissertation work.